Supreme Court, U.S.
FILED

091532 JUN 14 2010

OFFICE OF THE CLERK

IN THE
SUPREME COURT OF THE UNITED STATES

CHARLES CLAYTON, LIEUTENANT COLONEL,
UNITED STATES ARMY,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for Writ of Certiorari To the United States Court of Appeals for the Armed Forces

PETITION FOR WRIT OF CERTIORARI

MARK TELLITOCCI
Colonel, United States Army
Chief, Defense Appellate Division

JONATHAN POTTER
Lieutenant Colonel,
United States Army
Senior Appellate Counsel,
Defense Appellate Division

TIMOTHY THOMAS
Major, United States Army
Appellate Counsel
Defense Appellate Division

WILLIAM E. CASSARA
Appellate Counsel
Counsel of Record
PO Box 2688
Evans, Georgia 30809
707-860-5769
wcassara1@comcast.net

JESS ROBERTS
Captain,
United States Army,
Appellate Counsel
Defense Appellate
Division

Counsel for Petitioner

QUESTION PRESENTED

WHETHER PETITIONER'S FOURTH AMENDMENT RIGHT TO BE FREE FROM UNREASONABLE SEARCHES AND SEIZURES WAS VIOLATED WHEN A MILITARY JUDGE FOUND PROBABLE CAUSE TO SEARCH PETITIONER'S QUARTERS DESPITE A COMPLETE ABSENCE OF EVIDENCE THAT PETITIONER HAD DOWNLOADED OR POSSESSED ANY CHILD PORNOGRAPHY AND WHERE THERE WAS NO NEXUS OF ANY TYPE BETWEEN CHILD PORNOGRAPHY AND THE LOCATION SEARCHED.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

TABLE OF AUTHORITIES iii

OPINIONS BELOW 1

JURISDICTION 2

CONSTITUTIONAL PROVISION INVOLVED 2

STATUTE INVOLVED 2

MANUAL FOR COURTS-MARTIAL
PROVISION INVOLVED 4

STATEMENT OF THE CASE 5

Procedural History 5

Statement of Facts 6

REASONS FOR GRANTING THE WRIT 12

SUMMARY OF ARGUMENT 12

ARGUMENT 13

CONCLUSION 27

APPENDIX A - United States Army Court of Criminal Appeals Decision 1a

APPENDIX B - United States Court of Appeals for the Armed Forces Decision 4a

TABLE OF AUTHORITIES

CASES: *Page(s)*

Brinegar v. United States, 338 U.S. 160 (1949) 13

Brown v. Texas, 443 U.S. 47
(1979) 13

Illinois v. Gates, 462 U.S. 213
(1983) 11,14,21,25

United States v. Leon, 468 U.S. 897
(1984) 19

Wilson v. Layne, 526 U.S. 603
(1999) 13

Ybarra v. Illinois, 444 U.S. 85
(1979) 24

Zurcher v. Stanford Daily, 436 U.S. 547
(1978) 14

Poolaw v. Marcantal, 565 F.3d 721
(10th Cir. 2009) 14

United States v. Brown, 951 F.2d 999
(9th Cir. 1991) 24

United States v. Clayton, 68 M.J. 419
(C.A.A.F. 2010) 1,6,18,19,21,22,23,25

United States v. Coreas, 419 F.3d 151
(2d Cir. 2005) 23,24,25

United States v. Froman, 355 F.3d 882
(5th Cir. 2004) 19,20

United States v. Gonzalez, 399 F.3d 1225
(10th Cir. 2005) 14

United States v. Gourde, 440 F.3d 1065
(9th Cir. 2006) 19,20

United States v. Hutto, 84 Fed. App'x 6
(10th Cir. 2003) 19,20

United States v. Martin, 426 F.3d 68
(2d Cir. 2005) 19,20,23

United States v. Rubio, 727 F.2d 786
(9th Cir. 1984) 25

United States v. Weber, 923 F.2d 1338 (9th Cir. 1990) 24

CONSTITUTION, STATUTES, AND RULES FOR COURTS-MARTIAL: *Page(s)*

U.S. CONST. amend. IV 2,12,13,22,23,24,25

10 U.S.C. § 867(a)(3) (2005) 2

10 U.S.C. § 892 (2005) 2,3,5

10 U.S.C. § 934 (2005) 2,3,5

28 U.S.C. § 1259(3)(2005) 2

Manual for Courts-Martial 311(b)(3)(C)(2005) 5,19

Manual for Courts-Martial 315(f)(2)(2005) 4,15,21

IN THE
SUPREME COURT OF THE UNITED STATES

CHARLES CLAYTON, LIEUTENANT COLONEL,
United States Army, Petitioner,

v.

THE UNITED STATES OF AMERICA, Respondent

On Petition for a Writ of Certiorari
To the United States Court of Appeals for the Armed Forces

PETITION FOR WRIT OF CERTIORARI

The petitioner, Charles Clayton, respectfully prays that a writ of certiorari issue to review the decision of the United States Court of Appeals for the Armed Forces in this case.

OPINIONS BELOW

The opinion of the United States Army Court of Criminal Appeals is unpublished (Appendix A). The decision of the United States Court of Appeals for the Armed Forces is reported at 68 M.J. 419 (C.A.A.F. 2010) (Appendix B).

JURISDICTION

The judgment for the Court of Appeals for the Armed Forces (CAAF) was entered on March 17, 2010. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1259(3), the United States Court of Appeals for the Armed Forces having reviewed this case pursuant to Article 67(a)(3), Uniform Code of Military Justice (UCMJ); 10 U.S.C. § 867(a)(3).

CONSTITUTIONAL PROVISION INVOLVED

This case involves the Fourth Amendment to the United States Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

STATUTE INVOLVED

This case also involves Articles 92 and 134, UCMJ; 10 U.S.C. §§ 892 and 934. These sections are provided below:

10 U.S.C. § 892 (2005)

> Any person subject to this chapter who-
>
> (1) violates or fails to obey any lawful general order or regulation;
>
> (2) having knowledge of any other lawful order issued by a member of the armed forces, which it is his duty to obey, fails to obey the order;
>
> (3) is derelict in the performance of his duties, shall be punished as a court-martial may direct.

10 U.S.C. § 934 (2005)

> Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.

MANUAL FOR COURTS-MARTIAL PROVISION INVOLVED

MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 315(f)(2) provides in relevant part:

> (2) *Probable cause determination.* Probable cause to search exists when there is a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched. A search authorization may be based upon hearsay evidence in whole or in part. A determination of probable cause under this rule shall be based upon any of the following:
>
> (A) Written statement communicated to the authorizing officer;
>
> (B) Oral statements communicated to the authorizing official in person, via telephone, or by other appropriate means of communication; or
>
> (C) Such information as may be known by the authorizing official that would not preclude the officer from acting in an impartial fashion. The Secretary of Defense or the Secretary concerned may prescribe additional requirements.

MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 311(b)(3)(C) provides in relevant part:

> (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the issuance of the authorization or warrant. Good faith shall be determined on an objective standard.

STATEMENT OF THE CASE

Procedural History

On February 13, 2007, petitioner was tried by a military judge sitting as a general court-martial at Fort McPherson, Georgia. The military judge convicted petitioner, pursuant to his conditional pleas, of violating a lawful general order and wrongful possession of child pornography, in violation of Articles 92 and 134, UCMJ; 10 U.S.C. §§ 892 and 934. The military judge sentenced petitioner to confinement for forty months and a dismissal. Pursuant to the terms of the pretrial agreement, the convening authority approved only thirty-six months confinement, but otherwise approved the adjudged sentence. The convening authority also credited petitioner with seven days of confinement credit.

In a per curiam opinion dated May 9, 2008, the Army Court of Criminal Appeals (ACCA) amended the Specification of Charge I regarding the location of the offense, affirmed the amended specification and the balance of the findings, and affirmed the sentence. On June 16, 2008, petitioner filed a petition for grant of review with the CAAF and filed a supplement to the petition on July 31, 2008. On August 7, 2008, respondent filed an opposition to the petition without formal briefing.

On July 22, 2009, the CAAF granted review of the following issue:

> WHETHER THE MILITARY JUDGE ERRED IN DENYING APPELLANT'S MOTION TO SUPPRESS THE EVIDENCE SEIZED FROM APPELLANT'S QUARTERS.

The CAAF rendered its opinion on March 17, 2010, affirming the decision of ACCA in a 3-2 decision. The CAAF held that the military judge did not err in denying petitioner's motion to suppress evidence seized from petitioner's quarters.

Statement of Facts

On November 15, 2005, Senior Special Agent (SSA) Glen Watson, of the Department of Homeland Security's Immigration and Customs Enforcement Division (ICE), discovered an Internet child

pornography website group on Google entitled "Pre-Teen Bestiality and Anything Taboo" (Group). He reviewed various postings to the Group, including one picture of child pornography and several requests for various types of child pornography and child exploitation.

SSA Watson informed Google that a group operating on a Google website had posted child pornography. SSA Watson also requested information associated with the Group's moderator and "approved members." Google immediately shut down the website on November 15, 2005. Pursuant to a subpoena, Google provided ICE with a list of names and Internet addresses of approximately 130 members of the Group on February 16, 2006. The membership list included the e-mail address of "charlesjclayton@yahoo.com."

SSA Watson obtained information from Google and Yahoo identifying petitioner as the owner of the e-mail account bearing his name. SSA Watson discovered that petitioner's Yahoo account had been accessed via Internet Protocol (IP) and traced to a computer owned and operated by the U.S. Army in Kuwait. He learned that petitioner was a lieutenant colonel in the U.S. Army Reserve serving in Kuwait and that he had a residential address in Alpharetta, Georgia.

On March 8, 2006, SSA Watson prepared a detailed report of his investigation (ICE Report) and forwarded it to the Criminal Investigation Command

(CID) Headquarters in Baghdad, Iraq, and then to Kuwait for further investigation.

SSA Watson found no criminal conduct by petitioner, as per his ICE Report. His investigation showed only that, at some unknown time, petitioner registered for membership with the Group.

On April 18, 2006, CID Special Agent (SA) Yolanda McClain received SSA Watson's detailed ICE Report. She spoke with SSA Watson four or five times regarding the facts and status of the investigation. She verified that petitioner was assigned to Kuwait as a Safety Officer, the location of petitioner's quarters, and that he had recently departed for Hawaii for two weeks' leave.

SA McClain drafted an affidavit and request for search authorization to search petitioner's work computer and his room for a personal computer and any media storage devices. Most of the information in the two-page request for search authorization was taken verbatim from SSA Watson's ICE report. In an e-mail exchange with SA McClain, SSA Watson told her that it was possible that petitioner had received child pornography through the Group, but that it was impossible to determine how many times he accessed the Group's website.

SA McClain's affidavit stated that: "[t]he Camp Arifjan CID Office is currently conducting the discovery of apparent child pornography located within one of the Coalition Forces Land Component

Command (CFLCC) CAKU computers and the suspected login user is [Lieutenant Colonel (LTC)] Charles J. Clayton . . . ." The affidavit also stated that "[m]embership logs . . . indicated that LTC Clayton requested a 'Digest' for the Group, in which he would receive daily e-mails that would contain 25 of the postings to the Group sent as a single e-mail to his account . . . ."

SA McClain's affidavit also stated that ICE had recently executed two search warrants, resulting in the arrests of the Group's moderator and media manager.

After coordinating with the CFLCC Safety Office, CID conducted a search of petitioner's work area. His government-issued laptop was seized, as well as various DVDs and CDs. Sometime later, these items were sent to Germany for further investigation by CID computer analysts, who uncovered no incriminating evidence. The results of CID's analysis of the evidence seized from petitioner's workspace were not known for several weeks.

On April 20, 2006, SA McClain met with Major (MAJ) Lyons, the local military magistrate. She showed the magistrate her affidavit, the search authorization request, and SSA Watson's ICE Report. Both SA McClain and the military magistrate knew that petitioner resided in Building 507, which had wireless Internet access, but this fact was not presented in the affidavit. The material provided by SA McClain to the military magistrate

did not indicate how often petitioner had accessed the Group, if ever, nor did it indicate that he accessed the website from his quarters, or that he owned a personal computer.

The military magistrate reviewed the evidence, principally the ICE Report and SA McClain's affidavit. Later that afternoon, the military magistrate approved the search authorization.

SA McClain searched petitioner's quarters in Building 507. SA McClain discovered and seized three computers, 536 CDs and DVDs, three external hard drives, and other pieces of computer media. A search of the digital media revealed suspected child pornography images and videos, among other things.

On October 19, 2006, petitioner filed a timely motion to suppress the evidence seized in his quarters. Petitioner argued that there was no probable cause for the search authorization. Respondent filed a response on November 1, 2006. On January 9, 2007, the military judge conducted a pre-trial hearing on the motion to suppress. SSA Watson, SA McClain, and MAJ Lyons testified.

SA McClain testified that she wrote the following in her affidavit: "The Camp Arifjan CID Office is currently conducting the discovery of apparent child pornography located within one of the Coalition Forces Land Component Command (CFLCC) CAKU computers and the suspected login user is LTC Charles J. Clayton." She testified that she meant to

say in her affidavit that a military computer in Kuwait had accessed a Yahoo account through a U.S. Army server in Kuwait and that petitioner was a suspect because of his membership in the Group and his use of this Yahoo account.

SA McClain also testified that, based on her CID and law enforcement training, discussions with other CID agents, and prior experience with four or five Kuwait-based investigations regarding child pornography, she was aware that suspects who collect child pornography usually store the images on various media devices. She testified that SSA Watson told her about the arrests of the Group moderator and media manager.

The military judge denied petitioner's motion to suppress and issued written findings of fact and conclusions of law. The military judge concluded that the military magistrate had a substantial basis for concluding that probable cause existed to conduct the search, citing *Illinois v. Gates*, 462 U.S. 213 (1983). The military judge gave substantial deference to the magistrate's finding that probable cause existed to authorize the search. The military judge found that SSA Watson's ICE Report and SA McClain's affidavit established a fair probability that child pornography would be found in petitioner's quarters and media sources. The military judge also concluded, in the alternative, that the evidence was admissible under the good faith exception to the exclusionary rule.

Petitioner entered into a pretrial agreement with the convening authority, agreeing to plead guilty, with exceptions, to the charged offenses. The pretrial agreement preserved petitioner's motion to suppress for appeal. Petitioner was convicted and sentenced on February 13, 2007.

REASONS FOR GRANTING THE WRIT

Petitioner's constitutional right to be secure in his quarters against an unreasonable search without probable cause was violated. There was no probable cause to search petitioner's quarters and media sources because there was no actual nexus between the evidence sought and the place to be searched.

SUMMARY OF ARGUMENT

The Fourth Amendment requires a nexus between the evidence sought and the location to be searched. The trial judge and the appellate court erred when they upheld the military magistrate's ruling despite the complete absence of the presentation to the military magistrate of any information demonstrating the required nexus. Petitioner's subscription to an Internet group that advertises child pornography, without more, is insufficient to support probable cause to search a suspect's residence. Should this Court affirm the decision of the lower appellate court, servicemembers may be subjected to search and seizure based solely on associations or memberships without any evidence that a crime has been committed. The CAAF found

probable cause despite there being no evidence that petitioner ever accessed the Group following his initial subscription, or, that if he did, he accessed the Group from his quarters, that he downloaded any child pornography to his personal computer, or that he stored any images in his quarters. In doing so, the CAAF established a dangerous precedent—if an individual subscribes to an Internet group and that group is alleged to have an illegal purpose, the government has probable cause to obtain a warrant to search the subscriber's home even when there is no particularized evidence that the subscriber visited the Internet group subsequent to subscription or participated in the group's functions in any manner. Because the CAAF failed to make an individualized assessment of petitioner's participation, or lack thereof, the CAAF's holding violates the Fourth Amendment's protection against unreasonable searches and seizures.

ARGUMENT

All Americans, including petitioner, have a fundamental right to be free from "rash and unreasonable interferences with privacy and from unfounded charges of crime." *Brinegar v. United States*, 338 U.S. 160, 176 (1949); *see also Wilson v. Layne*, 526 U.S. 603, 610 (1999) ("The Fourth Amendment embodies this centuries-old principle of respect for the privacy of the home."); *Brown v. Texas*, 443 U.S. 47, 51 (1979) ("A central concern [is] . . . to assure that an individual's reasonable expectation of privacy is not subject to arbitrary

invasions solely at the unfettered discretion of officers in the field.").

"The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (abrogated by statute on other grounds). "[T]he necessity of a nexus between the suspected criminal activity and the particular place to be searched is so well established that in the absence of such a connection, 'the affidavit and resulting warrant are so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" *Poolaw v. Marcantal*, 565 F.3d 721, 734 (10th Cir. 2009) (quoting *United States v. Gonzalez*, 399 F.3d 1225, 1231 (10th Cir. 2005)).

In *Illinois v. Gates*, this Court explained that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." 462 U.S. 213, 232 (1983). "The task of the issuing magistrate or judge is simply to make a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime *will be found in a particular place*." *Id.* at 238 (emphasis added). In other words, there must be a nexus between the contraband or evidence sought and the place to be searched. *See Id.* Military Rule of Evidence

(M.R.E.), 315(f)(2) recognizes this nexus requirement, defining probable cause as "a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched."

The military magistrate relied principally on SSA Watson's ICE Report and SA McClain's affidavit to determine that probable cause existed to search petitioner's quarters and media storage devices. Examination of these documents reveals that there was no nexus between the evidence sought and petitioner's quarters.

SSA Watson's ICE Report explained how SSA Watson identified petitioner as a suspect but provided no evidence that petitioner had committed any offense. SSA Watson had perused several months of postings to the Group, many of which were photocopied and included in the ICE Report. Not one of these postings mentioned petitioner, was addressed to him, nor sent by him. The ICE Report stated that SSA Watson contacted Google the day he discovered the Group and that Google promptly shut down the Group. SSA Watson documented that, two months after contacting Google, he summoned Google to provide a membership list, which included petitioner's Yahoo e-mail address. SSA Watson requested that Yahoo inform him who had registered petitioner's Yahoo e-mail address, when the address had been most recently accessed, and from which IP address. SSA Watson determined that petitioner was the apparent registered owner of the e-mail

address; that he used the Yahoo account most recently via an IP address owned by the U.S. Army in Kuwait; that he opened the e-mail account from an IP address in Alpharetta, Georgia; and that petitioner was likely a servicemember.

SSA Watson's ICE Report failed to state that appellant had possessed or downloaded any child pornography. The ICE Report also failed to state that though it was possible that petitioner had received child pornography through the Group, it was impossible to determine how many times, if any other than requesting a digest, petitioner had accessed the Group. The ICE Report also failed to state that SSA Watson had advised SA McClain to subpoena Yahoo to determine how many times petitioner had accessed the Group. Notably, SSA Watson's ICE Report did not contain a profile of child pornography collectors.

SA McClain's one-and-a-half-page affidavit summarized her experience with "several computer crimes," including child pornography. She explained how SSA discovered the "Pre-teen Bestiality and Anything Taboo" Group and how she identified petitioner as a member. She concluded by stating that the moderator and media manager of the Group had been arrested and confessed to possessing a quantity of child pornography.

SA McClain's affidavit failed to inform the military magistrate that SSA Watson had advised her to subpoena Yahoo to determine how many times

petitioner had accessed the Group. The affidavit also failed to provide any information that petitioner had downloaded any child pornography from the Group or that he participated in any discussions, chats, or other activities as a Group member, save for his request to receive a digest. SA McClain failed to inform the magistrate that there had been no activity on the Group website for months as it had been shut down by Yahoo six months earlier. She had no evidence that petitioner received any digests or that, if he did, the digests contained child pornography. There was no evidence that petitioner used the wireless Internet access available in Building 507.

Not only did SA McClain's affidavit fail to establish a nexus between the possession of child pornography and petitioner's quarters, the affidavit contained a false statement. Though SA McClain wrote that petitioner apparently possessed child pornography on his government issued computer, this statement was false. No child pornography had been located on a CFLCC computer issued or used by petitioner.

In holding that probable cause to search petitioner's quarters exists, the CAAF added a fact not presented to or considered by the military magistrate. The CAAF wrote:

> In view of the ease with which laptop computers are transported from work to

> home and the ease with which computer media may be replicated on portable devices, the information provided to the magistrate was sufficient to support a practical, commonsense decision by the magistrate that there was a fair probability that contraband would be located in Appellant's quarters.

United States v. Clayton, 68 M.J. 419, 424-25 (C.A.A.F. 2010).

The CAAF held that the magistrate was not required to resolve matters such as whether petitioner posted messages to the Group, uploaded or downloaded child pornography, how long petitioner had belonged to the Group, how often petitioner had accessed the website, or whether he received the digests he requested for purposes of a probable cause determination. *Id.* at 425. Such actions "could have been taken to enhance law enforcement investigations as well as questions appropriately addressed to the factfinder at a court-martial in regard to whether the prosecution, at trial, could meet the high standard of proof beyond a reasonable doubt." *Id.*

The CAAF severed SA McClain's erroneous and misleading statement from the affidavit after concluding that the military magistrate did not consider it significant for the probable cause equation. *Id.* at 426. The CAAF held that the remaining information was "more than adequate to

demonstrate that the magistrate had a substantial basis for finding probable cause to search Appellant's quarters." *Id.* After severing the misleading statement, the CAAF chose not to consider the military judge's alternative holding under the good faith exception to the exclusionary rule. *Id. See* M.R.E. 311(b)(3)(C); *United States v. Leon*, 468 U.S. 897 (1984).

The CAAF relied upon cases from other courts in which "a person's voluntary participation in a website group that had as its purpose the sharing of child pornography supported a probable cause determination that child pornography would be found on the person's computer." *Clayton*, 68 M.J. at 424 (citing *United States v. Gourde*, 440 F.3d 1065, 1072-73 (9th Cir. 2006) (en banc); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004); *United States v. Hutto*, 84 Fed. App'x 6, 8 (10th Cir. 2003)). According to the CAAF, "[t]hese cases reflect a practical, commonsense understanding of the relationship between the active steps that a person might take in obtaining child pornography from a website and retaining it for an extended period of time on that person's computer." *Clayton*, 68 M.J. at 424.

The cases cited by the CAAF majority are inapposite to the instant case. In *Gourde*, that defendant paid $19.95 per month for over two months to access a website containing child pornography images. 440 F.3d at 1067-68. He likely

paid by credit card and completed a multi-step process to enter his personal and financial information on the website. It is reasonable to assume that an individual who pays for a service is more likely to use that service in order to maximize the return on the investment than an individual who merely clicks on a "subscribe" button. *See id.* at 1070. Gourde did not become a member by accident or by a click of the computer mouse button. *Id.*

The affidavits in *Gourde*, *Martin*, and *Froman*,[1] all listed a behavioral profile of child pornography collectors and detailed the use of computers and other media storage devices by such collectors. 440 F.3d at 1068; 426 F.3d at 72; 355 F.3d at 889. Neither SSA Watson's ICE Report nor SA McClain's affidavit contained a behavioral profile of child pornography collectors or details regarding the use of computers and other media storage devices by such collectors. In *Gourde*, *Martin*, and *Froman*, the investigator sought to link those defendants' suspected possession of child pornography to characteristics common to such perpetrators. In petitioner's case, there was no such attempt to characterize him as a collector of child pornography or to explain how such collectors store and maintain depictions of child pornography.

---

[1] The *Hutto* court issued a very brief decision that did not discuss the contents of the affidavit in question. *United States v. Hutto*, 84 Fed. App'x 6 (10th Cir. 2003). The affidavit in *Hutto* was the same as the affidavits in *Martin* and *Froman*, as all three cases resulted from an investigation by FBI Special Agent Binney.

In the petitioner's case, two of the CAAF judges dissented from the majority's holding. *Clayton*, 68 M.J. at 426 (Ryan, J. and Erdmann, J., dissenting.) The dissenting judges recognized that other circuit courts had reached similar conclusions as the majority, "[b]ut that others have joined our adventures does not make the course any less a folly. The better route is to continue to require, consistent with both M.R.E. 315(f)(2) and *Gates*, 462 U.S. at 238, some nexus between the items sought and the place the government wants to search." *Id.* at 428. (citations omitted.)

The dissenters rejected the majority's reasoning because the military magistrate was not presented with any evidence that petitioner had signed up for wireless Internet service in his barracks or that the wireless Internet connection was routed through the Army server from which petitioner's Yahoo e-mail address had been accessed. *Id.* at 427. Judge Ryan, who authored the dissent, reasoned that petitioner could have checked his personal e-mail at work or at other locations where deployed servicemembers access the Internet. *Id.* She disagreed with the majority's reasoning that, because petitioner's government issue computer was a laptop, it was more likely that he stored child pornography in his quarters, as opposed to another location. *Id.* She wrote, "[t]he portability of both laptops and the digital movies and images the Government sought here makes any 'commonsense' link to Appellant's room exceedingly tenuous." *Id.*

Judge Ryan believed that the CAAF's decision had diluted the "requirement that there be an actual, as opposed to an intuitive or a hypothetical, nexus between the evidence sought and the location to be searched." *Id.* at 426. She wrote:

> The [CAAF] today appears to champion the idea that there is something *de minimis* about the Fourth Amendment's requirements when the thing sought by a search authorization or warrant is child pornography. It is now effectively the case that signing up for a website related to that topic-expressing an interest in it, from any location at all-provides sufficient cause to search one's home or living quarters. . . . This reasoning requires three logical inferences: First, if the suspect is a member of an Internet group related to child pornography, he has access to a computer. Second, if he has access to a computer, it is in his home or living quarters. Third, membership in the group equates to downloading and possessing child pornography. The first inference makes sense, but the other two do not—at least on the evidence presented to this magistrate. Once we have held that an expressed interest in child pornography probably means you are viewing and secreting it *somewhere*, it seems equally sustainable to hold

> that the government is free to search for that pornography *anywhere*. This comes dangerously close to revising the writs of assistance that were the impetus for enacting the Fourth Amendment in the first place.

Id. at 428. (citation omitted).

Judge Ryan's analysis does not stand alone, but is supported by decisions from both the Second and the Ninth Circuits. In two recent cases, the Second Circuit held that the defendants' memberships in online child pornography e-groups were sufficient to establish probable cause for obtaining search warrants of their computers and homes. *See United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005); *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005). The cases were factually similar, but *Coreas* was decided by a different panel than in *Martin*. The *Coreas* panel unanimously agreed with Judge Pooler's dissent in *Martin* that the evidence was insufficient to establish probable cause where the government failed to demonstrate that Martin had downloaded child pornography and that the corrected affidavit supported only the inference that he had used legal, text-based functions of the website outside the purview of prohibited activity. *Coreas*, 419 F.3d. at 159. The *Coreas* panel upheld that defendant's conviction only because of the precedent established by *Martin*. *Id.*

In *United States v. Weber*, the court held that the trial court should have suppressed the evidence of child pornography seized pursuant to a search warrant. 923 F.2d 1338 (9th Cir. 1990). Regarding the logical leaps the trial court took to determine that probable cause existed, the Court reasoned:

> But with each succeeding inference, the last reached is less and less likely to be true. Virtual certainty becomes probability, which merges into possibility, which fades into chance. The Fourth Amendment requires a "fair probability" that the items searched for will be found."

Id. at 1344-45 (citation omitted).

The CAAF's holding appears to reflect society's disgust with child pornographers and sexual predators. Such disgust with those who prey upon the most innocent members of our society is understandable, but this disgust should not permit an end run around the Fourth Amendment. Though the Group may have provided a forum for a repugnant viewpoint, this does not alone support an inference of criminal conduct. *Coreas*, 419 F.3d at 156. The *Coreas* court stated that a "'person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search . . . .'" *Id.* (quoting *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979)). *See United States v. Brown*, 951 F.2d 999, 1003 (9th Cir. 1991) (ruling

that individual police officer's membership in a corrupt police unit was not sufficient for probable cause without further proof that the officer actually participated in illegal activities); *United States v. Rubio*, 727 F.2d 786, 793-94 (9th Cir. 1984) (holding that membership in Hell's Angels, without more, was not sufficient for probable cause without particularized allegation that the individual participated in the organization's criminal activity). The majority suggests that because the Group's moderator and media manager confessed to possessing child pornography, then petitioner must have possessed child pornography.

The CAAF majority erroneously attempts to create the required nexus between petitioner and illegal activity by appealing to "commonsense." *Clayton*, 68 M.J. at 424. The majority is correct that a military magistrate presented with a warrant may "make a practical, common sense decision," but that decision must be based on the "circumstances set forth in the affidavit." *Gates*, 462 U.S. at 238. Here, the affidavit fails to establish a sufficient nexus between petitioner and possessing child pornography. Respondent only offered evidence that petitioner clicked on a button to subscribe to the Group. As the *Coreas* court concluded, "[t]he notion that, by this act of clicking a button, [the defendant] provided probable cause for the police to enter his private dwelling and rummage through [his] various . . . personal effects seems utterly repellent to core purposes of the Fourth Amendment." 419 F.3d. at 156.

A subscription to an Internet group that advertises child pornography, without more, is insufficient to support probable cause to search a suspect's residence. Without the need for a nexus between the illegal activity and the place to be searched, one can imagine that the CAAF would find probable cause where an individual might mistakenly click a "subscribe" button in a pop-up ad on a website, or where a concerned parent subscribed to an Internet group to better understand the potential threats to his or her children, or where an individual subscribes to such a website for legitimate research purposes. Should the CAAF holding stand, servicemembers may be subjected to searches and seizures based solely on association or membership without any evidence that these servicemembers have committed a crime.

CONCLUSION

WHEREFORE, petitioner respectfully requests that this Court grant his petition.

Respectfully submitted,

MARK TELLITOCCI
Colonel, United States Army
Chief,
Defense Appellate Division

JONATHAN POTTER
Lieutenant Colonel,
United States Army
Senior Appellate Counsel,
Defense Appellate Division

TIMOTHY THOMAS
Major, United States Army
Appellate Counsel
Defense Appellate Division

WILLIAM E. CASSARA
Appellate Counsel
Counsel of Record
PO Box 2688
Evans, GA 30809
707-860-5769
wcassara1@comcast.net

JESS B. ROBERTS
Captain,
United States Army
Appellate Counsel
Defense Appellate Division

Counsel for Petitioner

APPENDIX A

UNITED STATES ARMY COURT

OF CRIMINAL APPEALS

ARMY 20070145

UNITED STATES, Appellee

v.

Lieutenant Colonel Charles J. CLAYTON
United States Army, Appellant

Appeal from the Army Court of Criminal Appeals

Decided May 9, 2008

Before: Holden, Hoffman and Sullivan, Judges

SUMMARY DISPOSITION

Per Curiam:

This case is before us for review under Article 66, Uniform Code of Military Justice, 10 U.S.C. §866 [hereinafter UCMJ]. We find error in the findings of the court-martial as described below.

In the Specification of Charge I, appellant was charged with violation of lawful general orders by, *inter alia,* wrongful possession of adult and child pornography at Camp Arifjan and Camp Doha, Kuwait, in violation of Article 92, UCMJ. Appellant's providence inquiry does not support his plea to the Camp Doha situs. Accordingly, we set aside the finding of guilty to and dismiss only so much of the Specification of Charge I as states, "and at or near Camp Doha, Kuwait" and affirm the finding of guilty to the specification as amended.

The remaining findings of guilty are affirmed. We have considered the assignments of error and find them to be without merit. Reassessing the sentence on the basis of the error noted, the entire record, and applying the principles of *United States v. Sales,* 22 M.J. 305 (C.M.A. 1986) and *United States* v. *Moffeit,* including Judge Baker's concurring opinion, 63 M.J. 40,43 (C.A.A.F. 2006), the court affirms the sentence.*

FOR THE COURT

/s/ MALCOM H. SQUIRES

---

* On 1 May 2008, we denied a defense motion for an 11 June 2008 oral argument, which claimed "[counsel] needs the requested time to complete his previously scheduled active duty training and to properly prepare for oral argument." This court previously granted appellant's "Motion for Expedited Review" in this case, which averred "neither claim [assignment of error] is novel or unusually complex." Consistent with appellant's request for expedited review and our superior court's mandate, we issued a decision as expeditiously as possible while safeguarding appellant's rights under Article 66, UCMJ. *See United States v. Moreno*, 63 M.J. 129, 135 (C.A.A.F. 2006) (reviewing claims of post-trial and appellate delay using the four-factor analysis in *Barker v. Wingo*, 407 U.S. 514 (1972)); *see also United States v. Finch*, 64 M.J. 118, 125 (C.A.A.F. 2006) (noting appellant's request for expedited review in evaluating appellant's claim of dilatory post-trial processing).

APPENDIX B

UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

No. 08-0644

UNITED STATES, Appellee

v.

Charles J. CLAYTON, Lieutenant Colonel, U.S. Army, Appellant

Appeal from the Army Court of Criminal Appeals

Argued November 17, 2009.
Decided March 17, 2010.

Before: Effron, C.J., delivered the opinion of the Court, in which Baker and Stucky, JJ. joined. Ryan, J., filed a dissenting opinion, in which Erdmann, J. joined.

Chief Judge EFFRON delivered the opinion of the Court:

A general court-martial composed of a military judge sitting alone convicted Appellant, pursuant to his conditional pleas, of violating a lawful general order and possession of child pornography, in violation of Articles 92 and 134, Uniform Code o f Military Justice (UCMJ), 10 U.S.C. § § 892, 934 (2006). The sentence adjudged by the court-martial included confinement for forty months and a dismissal. The convening authority approved a sentence that included confinement for thirty-six months and a dismissal, and provided the accused with seven days confinement credit. The convening authority also waived automatic forfeitures for a period of time with direction that the funds be paid to the wife of the accused. The United States Army Court of Criminal Appeals in a per curiam opinion amended the Specification of Charge I with respect to the location of the offense, affirmed the amended specification and the balance of the findings, and affirmed the sentence. United States v. Clayton, No. ARMY 20070145, 2008 CCA LEXIS 599, at *1 (A. Ct. Crim. App. May 9, 2008) (unpublished).

On Appellant's petition, we granted review of the following issue:

> WHETHER THE MILITARY JUDGE ERRED IN DENYING APPELLANT'S MOTION TO SUPPRESS THE EVIDENCE SEIZED FROM APPELLANT'S QUARTERS.

For the reasons set forth below, we affirm.

I. BACKGROUND

The present appeal concerns a search conducted during a child pornography investigation. Based upon information provided by law enforcement personnel from the United States Army Criminal Investigation Command (CID) agents, a military magistrate authorized a search of Appellant's quarters. The information provided to the magistrate included details concerning Appellant's subscription to an Internet group formed to discuss, share, and distribute child pornography, his communication with the group, identifying data about his e-mail account, and other related information. When the CID agents conducted a search of Appellant's quarters, they found a personal computer and digital media that contained thousands of images of child pornography, which formed the basis for the charges at issue in the present appeal.

Prior to trial, Appellant moved to suppress the seized evidence asserting a lack of probable cause for the search. The military judge denied the motion. Appellant entered a plea of guilty while preserving the right to appeal the military judge's ruling.

A. THE MILITARY JUDGE'S FINDINGS OF FACT

The following summarizes the military judge's findings of fact on the suppression motion, as well as information provided to the magistrate by CID

Special Agent (SA) Yolanda McClain, who was stationed in Kuwait and assigned investigative responsibilities for the case. The events at issue occurred during the period in which Appellant served as a mobilized United States Army Reserve Officer in Kuwait. The initial investigation was conducted by Senior Special Agent (SSA) Glen Watson, an investigator with the Investigations Division of the Office of Homeland Security Immigration and Customs Enforcement (ICE) . SSA Watson worked in the Child Exploitation Unit, where his duties included investigating child pornography and exploitation. In the course of his duties, SSA Watson discovered an Internet child pornography website group on Google entitled, "Preteen-Bestiality-and-Anything-Taboo." During the investigation, SSA Watson discovered a picture of child pornography that had been posted on the site. He also found several requests for various types of child pornography and other requests for child exploitation.

SSA Watson contacted Google, informing them that a group operating on a Google site had posted child pornography. SSA Watson also requested information associated with the group's moderator and "approved members." In response, Google shut down the site. Google also provided ICE with a list identifying the members of the "Preteen-Bestiality-and-Anything-Taboo" group by subscriber notification category and e-mail address. The membership list of the "Preteen-Bestiality-and-Anything-Taboo" group included an e-mail account bearing his name, "charlesjclayton@yahoo.com."

During the investigation, SSA Watson obtained information from Google and Yahoo that identified Appellant as the owner of the e-mail account bearing his name, "charlesjclayton@yahoo.com." In response to a subpoena, Yahoo provided Appellant's login name and an alternate e-mail address associated with Appellant's civilian employer.

SSA Watson used the information he gathered and an Internet protocol address to ascertain that Appellant's Yahoo account had been accessed from a computer owned and operated by the United States Army in Kuwait. Additionally, SSA Watson conducted an Internet search and found an article entitled "Roads traveled in Kuwait bring concern" by a "Lieutenant Colonel Charles Clayton."

SSA Watson was able to identify Appellant as a subscriber to the site who had asked the group's moderator to provide him with digest notification privileges. Specifically, Appellant requested automatic transmission to his Yahoo account by e-mail of up to twenty-five postings each day.

SSA Watson prepared a detailed report of his investigation, which was forwarded through military channels to SA McClain. SA McClain used this information to prepare a request for search authorization, including a supporting affidavit.

SA McClain summarized the results of SSA Watson's investigation in the affidavit. The affidavit described the activities of "an internet group on Google called 'Preteen-Bestiality-and-Anything-

Taboo.'" According to the affidavit, members of the group used the website "to share child pornography pictures, videos, and exploitation information amongst themselves." The affidavit stated that "[m]embership logs ... indicated that LTC CLAYTON requested a 'Digest' for the [g]roup, in which he would receive daily e-mails that would contain 25 of the postings to the [g]roup sent as a single e- mail to his account ...". With respect to Appellant, the affidavit stated that as a recipient of the digest, "it is possible that he [Appellant] was the recipient of child pornography directly to his Yahoo e-mail account ..."

The affidavit also stated that ICE recently had executed two search warrants, resulting in the arrests of two members of the group. One of the members, the moderator of the group, confessed to "possessing a large quantity of child pornography." The other member, the individual who "actually uploaded the child pornography to the [g]roup also ... confessed and was arrested."

The affidavit stated that the government had furnished Appellant with a laptop computer, providing the model and serial number. SA McClain requested permission to search for media files concerning child pornography on the laptop, in Appellant's quarters, and in Appellant's workspace.

On April 20, 2006, SA McClain met with the local military magistrate and briefed him on the status of the investigation. SA McClain provided the magistrate with the affidavit, the search authorization request, and the ICE Report. SA

McClain and the magistrate were aware that Appellant lived in a single person room in Building 507, which had wireless Internet service capability. The material provided by SA McClain to the magistrate did not indicate how often Appellant accessed the group site, nor did it indicate that he accessed the site from his quarters or that he owned a personal computer.

Following the interview with SA McClain, the magistrate reviewed the evidence and various sources of law. Later in the afternoon, he approved SA McClain's request to search Appellant's quarters.

B. THE MILITARY JUDGE'S CONCLUSIONS OF LAW

At trial, the military judge held that the magistrate had a substantial basis for concluding that probable cause existed to conduct the search, citing *Illinois v. Gates*, 462 U.S. 213, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). In reaching this conclusion, the military judge gave substantial deference to the magistrate's finding that probable cause existed to authorize the search, citing *United States v. Maxwell*, 45 M.J. 406, 423 (C.A.A.F. 1996).

The military judge stated that the evidence, principally from SSA Watson's ICE Report and SA McClain's affidavit, established a fair probability that child pornography would be found in Appellant's personal quarters and media sources. The military judge noted that the information was provided by an

experienced federal investigator from the Department of Homeland Security who specialized in investigating child pornography and child predators.

The military judge also concluded, in the alternative, that the evidence was admissible under the good faith exception to the exclusionary rule. *See* Military Rule of Evidence (M.R.E.) 311 (b) (3) (C); *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

II. REVIEW OF PROBABLE CAUSE DETERMINATIONS

We review a military judge's denial of a motion to suppress for an abuse of discretion. *United States v. Leedy*, 65 M.J. 208, 212 (C.A.A.F. 2007). An abuse of discretion occurs when we determine that the military judge's findings of fact are clearly erroneous or that he misapprehended the law. *Id.* at 213. In addressing the granted issue, we consider whether the military judge abused his discretion when he ruled as a matter of law that there was a substantial basis for finding probable cause existed under M.R.E. 315 (f) (2). *See id.* at 212 (citing *United States v. Rader*, 65 M.J. 30, 32 (C.A.A.F. 2007)). "[We] review the legal question of sufficiency for finding probable cause de novo using a totality of the circumstance test." *Id.* (citing *United States v. Reister*, 44 M.J. 409 (C.A.A.F. 1996)).

M.R.E. 315 (f) (2) defines probable cause as "a reasonable belief that the person, property, or evidence sought is located in the place or on the

person to be searched." In *United States v. Macomber*, 67 M.J. 214, 218 (C.A.A.F. 2009), we recently summarized the framework for reviewing probable cause determinations under M.R.E. 315.

The analysis focused on four key principles. First, determinations of probable cause made by a neutral and detached magistrate are entitled to substantial deference. *Id.* (quoting *United States v. Carter*, 54 M.J. 414, 419 (C.A.A.F. 2001)). Second, resolution of doubtful or marginal cases should be largely determined by the preference for warrants, and "'[c]lose calls will be resolved in favor of sustaining the magistrate's decision.'" *Id.* (quoting *United States v. Monroe*, 52 M.J. 326, 331 (C.A.A.F. 2000)) (alteration in original). Third, "courts should not invalidate [warrants] by interpreting [affidavits] in a hypertechnical, rather than a commonsense, manner." *Id.* (quoting *Gates*, 462 U.S. at 236, 103 S.Ct 2317)) (alteration in original) . Fourth, the evidence must be considered in the light most favorable to the prevailing party. *Reister*, 44 M.J. at 413.

We also have observed that "probable cause determinations are inherently contextual, dependent upon the specific circumstances presented as well as on the evidence itself." *Leedy*, 65 M.J. at 213. In *Leedy*, we emphasized that "probable cause is founded not on the determinative features of any particular piece of evidence provided an issuing magistrate ... but rather upon the overall effect or weight of all factors ..." *Id.*

In a particular case, the contextual circumstances may involve the timing of the determination and the nexus between the alleged criminal activity and the place searched. The question of timing focuses on the information presented to the search authority, as well as information known by the search authority, at the time the decision to search was made. *See* M.R.E. 315 (f) (2); *United States v. Cunningham*, 11 M.J. 242, 243 (C.M.A. 1981). The question of nexus focuses on whether there was a "fair probability" that contraband or evidence of a crime will be found in a particular place. *Leedy*, 65 M.J. at 213 (quoting *Gates*, 462 U.S. at 238, 103 S.Ct. 2317)) (quotation marks omitted) The nexus between the items to be seized and the place to be searched need not be based on direct observation but can be inferred from the facts and circumstances of a particular case. *See United States v. Lopez*, 35 M.J. 35, 38-39 (C.M.A. 1992). Determinative factors include the type of crime, the nature of the items sought, the extent of the suspect's opportunity for concealment, and normal inferences as to where a criminal would likely hide the property. *Id.*; *see United States v. Gallo*, 55 M.J. 418, 422 (C.A.A.F. 2001).

II. DISCUSSION

A. THE MAGISTATE'S PROBABLE CAUSE DETERMINATION

A number of courts have observed that a person's voluntary participation in a website group that had as its purpose the sharing of child pornography supported a probable cause determination that child pornography would be found on the person's

computer. *See United States v. Gourde*, 440 F.3d 1065, 1072-73 (9th Cir. 2006) (en banc); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004); *United States v. Hutto*, 84 Fed. Appx. 6, 8 (10th Cir. 2003). These cases reflect a practical, commonsense understanding of the relationship between the active steps that a person might take in obtaining child pornography from a website and retaining it for an extended period of time on that person's computer.

In the present case, the information provided to the magistrate identified Appellant as a member of a website group, "Preteen-Bestiality-and-Anything-Taboo." The group used the website to share child pornography and exploitation information. The moderator of the website group and the media manager had been arrested and had confessed to possession and distribution of child pornography. Appellant voluntarily joined the group and specifically requested digest notification, which enabled him to receive up to twenty-five postings sent in a single email automatically each day from the group to the e-mail account bearing his name, "charlesjclayton@yahoo.com." The e-mail account bearing his name had been accessed by a government computer in Kuwait. Appellant, who was stationed in Kuwait, had been provided with a laptop computer by the Army.

In short, the magistrate had information indicating that Appellant was a member of a group that shared Internet child pornography. The

information also indicated that Appellant had requested e-mail transmissions from the group, that Appellant used an e-mail account bearing his name to access the group, and that the same e-mail address had been accessed from Kuwait. In addition, the information indicated that Appellant possessed a laptop computer in Kuwait. In view of the ease with which laptop computers are transported from work to home and the ease with which computer media may be replicated on portable devices, the information provided to the magistrate was sufficient to support a practical, commonsense decision by the magistrate that there was a fair probability that contraband would be located in Appellant's quarters.

Appellant contends that the information before the magistrate was not sufficient to establish probable cause because no evidence showed that he posted messages to the Google site, participated in discussions, or uploaded or downloaded child pornography. Appellant also notes that the evidence before the magistrate did not indicate how long he belonged to the group, how often he accessed the website, or whether he received the digests he requested. He further notes that SA McClain never followed up on a suggestion from SSA Watson that she review his e-mail accounts to ascertain whether they contained such information.

The foregoing matters all involve actions that could have been taken to enhance the law enforcement investigation, as well as questions appropriately addressed to the fact finder at the court-martial in regard to whether the prosecution,

at trial, could meet the high standard of proof beyond a reasonable doubt. The magistrate, however, was not required to resolve these matters for purposes of making a probable cause determination with respect to a search authorization. The information presented to the magistrate regarding the activities of a voluntary member of the "Preteen-Bestiality-and-Anything-Taboo" web group was sufficient to support a search of his quarters.

B. IMPACT OF ERRONEOUS INFORMATION IN AN AFFIDAVIT

Appellant also contends that the information provided to the magistrate was tainted because SA McClain erroneously informed the magistrate that child pornography had been located on Appellant's government computer. Applying the corrective principle identified in *United States v. Cowgill*, after setting aside the erroneous information in an affidavit, "'there remains sufficient content in the warrant affidavit to support a finding of probable cause ....' " 68 M. J. 388, 392 (C.A.A.F. 2010) (quoting *Franks v. Delaware*, 438 U.S. 154, 171-72 (1978)).

In testimony before the military judge during the suppression hearing, SA McClain acknowledged that she had been in error. She meant to say that the suspect was within the command, not that they had located child pornography on Appellant's computer. SA McClain further testified that she addressed this misstatement during her meeting with the magistrate.

The military judge noted this misstatement in his findings of fact:

> Agent McClain stated in her affidavit that, "The Camp Arifjan CID Office is currently conducting the discovery of apparent child pornography located within one of the [Government's]...computers and the suspected login user is LTC Charles J. Clayton ...." This was not correct. No apparent child pornography had been located within a [Government] ... computer relating to LTC Clayton. Agent McClain later testified that she meant to say in the affidavit that a military computer in Kuwait had accessed a Yahoo account through a U.S. Army server in Kuwait and that LTC Clayton was a suspect because of his membership in the group and his use of this Yahoo account.

Although the military judge did not address expressly in his findings of fact whether, or to what extent, the magistrate considered SA McClain's explanation, the military judge set forth SA McClain's experience and stated: "She appeared to be a thorough investigator who did things based on her CID training and not out of malice or intent to take down a senior officer." In his conclusions of law, the military judge specifically stated that "Agent McClain did not act with any 'reckless' disregard for the truth." With respect to the magistrate's reliance

on the affidavit, the military judge concluded that the magistrate "did not in any sense abandon his judicial role, nor was he a 'rubber stamp' for the government." The military judge added that "[t]he affidavit was based on information provided by an experienced federal investigator, and it was not facially deficient." The military judge was in the best position to observe the person presenting information that supplemented the affidavit, assess credibility, and determine whether the misstatement constituted a reckless disregard for the truth. *See United States v. Rogers*, 67 M.J. 162, 166 (C.A.A.F. 2009) (relying on the military judge's assessment of information provided by a law enforcement agent in addition to the information in the agent's affidavit). Moreover, the military judge's findings of fact and conclusions of law demonstrate that the erroneous statement did not constitute a significant element of the probable cause equation. If we sever the erroneous statement from the affidavit, the remaining information before the magistrate, as set forth *supra* in Part I.A., was more than adequate to demonstrate that the magistrate had a substantial basis for finding probable cause to search Appellant's quarters. In view of our conclusion in that regard, we need not discuss the military judge's alternative holding under the good faith exception.

III.CONCLUSION

The decision of the United States Army Court of Criminal Appeals is affirmed.

RYAN, J., with whom ERDMANN, J., joins (dissenting)

I cannot agree with the continued dilution of the requirement that there be an actual, as opposed to an intuitive or a hypothetical, nexus between the evidence sought and the location to be searched. *Compare United States v. Higgins*, 557 F.3d 381, 390 (6th Cir. 2009) (finding no probable cause to search suspect's home because affidavit only stated that informant had purchased contraband from suspect and did not assert informant had ever been in suspect's home), *and United States v. Frazier*, 423 F.3d 526, 533 (6th Cir. 2005) (finding no probable cause because "the defendant's status as a drug dealer, standing alone, [does not] give rise to a fair probability that drugs will be found in his home"), *with United States v. Clayton*, 68 M.J. at 424-26 (C. A. A. F. 2010) (finding probable cause to search suspect's residence despite no evidence linking child pornography to that location), *United States v. Macomber*, 67 M.J. 214, 219-20 (C.A.A.F. 2009) (same), *and United States v. Gallo*, 55 M.J. 418, 422 (C.A.A.F. 2001) (same). Absent such dilution, the magistrate's finding of probable cause is not sustainable.

I. Probable Cause

"Probable cause to search exists when there is a reasonable belief that the ... evidence sought is located *in the place ... to be searched*." Military Rule of Evidence (M.R.E.) 315 (f) (2) (emphasis added); *accord Illinois v. Gates*, 462 U.S. 213, 238 (1983) (defining probable cause as "a fair probability that

contraband or evidence of a crime will be found in a *particular* place" (emphasis added)). This definition contemplates some nexus between the contraband or evidence sought and the place the government wants to search. *See United States v. Hall*, 50 M.J. 247, 250 (C.A.A.F. 1999).

In this case, a warrant was issued to search Appellant's barracks room for child pornography. In finding what it asserts to be the required nexus here, the majority relies on the following evidence:

1. That Appellant was a member of a Google Internet group called "Preteen-Bestiality-and-Anything-Taboo." 68 M.J. at 424-25.

2. That Appellant had specifically requested membership in the group and his membership level provided him with a single daily e-mail containing up to twenty-five new postings to the group. *Id.*

3. That both child pornography and information regarding child exploitation had been uploaded to the group in the past. *Id.* at 424.

4. That the moderator and media manager of the group had been arrested and confessed to possessing child pornography. *Id.* at 424-25.

5. That the e-mail account through which Appellant received messages from the Google group "had been accessed by a government computer in

Kuwait,"[1] the country in which Appellant was stationed. *Id.*

6. That Appellant's government computer was a laptop. *Id.*

The majority also notes that wireless Internet access was available in Appellant's dormitory, though it is unclear whether that factors into its probable cause analysis.[2] *Compare id.* at 423 (noting

---

[1] At this point the Government only knew that the account had been accessed by way of a U.S. Army *server* in Kuwait. It had no information regarding which computer had accessed the account. The affidavit ambiguously asserted that "[t]he *charlesjclayton@yahoo.com* account was accessed via Internet protocol (IP) address 143.81.248.47 which was traced to a computer that was owned and operated by the U.S. Army in Kuwait."

[2] The affidavit presented to the magistrate contained no information regarding wireless Internet access. And while both the magistrate and the affiant were independently aware that wireless access was available in the building, it is unclear whether that information was discussed or considered during the search authorization process -- the magistrate appears to have known wireless Internet was available not because of information presented in the course of reviewing the search authorization request, but because he had been involved in soliciting the contract for its installation and knew someone who used it. It is therefore at least an open question whether it was proper for him to consider this information in granting the search authorization. *See United States v. Leedy*, 65 M.J. 208, 214 (C.A.A.F. 2007) (stating that our probable cause analysis focuses on "the evidence as set out *in the four corners of the requesting affidavit* ... illuminated by factors such as the veracity, reliability, and basis of knowledge of the individual presenting the evidence") (emphasis added) (citations and quotation marks omitted); *see also Whiteley v. Warden, Wyo. State Penitentiary*, 401 U.S. 560, 565 n. 8 (1971) ("[A]n

both affiant and magistrate were aware wireless Internet access was available), *with id.* at 424-25 (discussing magistrate's probable cause determination without noting availability of wireless Internet).

Nothing in these facts provided the magistrate with the necessary nexus between the place to be searched -- Appellant's dorm room -- and the evidence sought. "The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978) (abrogated by statute on other grounds). But all these facts show is that there was ample probable cause to believe Appellant had *access* to child pornography. There is nothing to raise a reasonable belief that such pornography would be *in his quarters in Kuwait.*

Though wireless Internet access was generally available in Appellant's building, the magistrate was not presented with any evidence that Appellant signed up for such a connection or that the wireless Internet connection was routed through the Army server from which Appellant's

---

otherwise insufficient affidavit cannot be rehabilitated by testimony concerning information possessed by the affiant when he sought the warrant but not disclosed to the issuing magistrate.").

charlesjclayton@yahoo.com e-mail address had been accessed. *Cf. Macomber*, 67 M.J. at 221 (Ryan, J., dissenting) (finding no probable cause in part because affidavit contained no evidence accused actually owned a computer or had Internet access in his room). Appellant could have checked his personal e-mail at work, or at other locations where deployed servicemembers access the Internet. Likewise, the fact that his government-issued computer was a laptop did not make it any more likely that he was storing child pornography in his quarters, as opposed to somewhere else. *Cf. United States v. Rowland*, 145 F.3d 1194, 1205 (10th Cir. 1998) (finding no probable cause to search suspect's home because contraband videotapes were delivered to a post office box and "[h]is home ... was but one of an otherwise unlimited possible sites for viewing or storage ... [and t]he ... affidavit provided no basis to either limit the possible sites or suggest that [the suspect]'s home was more likely than the otherwise endless possibilities") . The portability of both laptops and the digital movies and images the Government sought here makes any "commonsense" link to Appellant's room exceedingly tenuous.

I dissented in *Macomber* because I did not believe the evidence there provided a legitimate nexus to the Appellant's dormitory room. 67 M. J. at 221-23 (Ryan, J., dissenting). But the magistrate in that case at least had in front of him a generic "pedophile profile," which indicated that persons with a sexual interest in children often store child pornography in

their homes (and especially in their bedrooms). Here, the magistrate was not presented with even this constitutionally minimally relevant evidence.[3]

Further, the magistrate in *Macomber* at least knew that the suspect had used his dormitory as the return address when ordering child pornography through the mail. 67 M.J. at 219. In this case, the only residence tied to child pornography was Appellant's residence in Georgia, the address associated with the charlesjclayton@yahoo.com account.

The facts here do not approach even the low bar this Court set in *Gallo*. In that case, child pornography had been found on the appellant's work computer and there was evidence that those files had been accessed from or copied to a floppy disk, leading the Court to reason that the floppy disk would likely be found at the suspect's home. 55 M.J. at 421-22; *id.* at 423 (Sullivan, J., concurring). In this case there was no evidence that Appellant had transferred pornography to media that he might have taken to his quarters, and no computer under Appellant's control had yet been found to contain child pornography.

The Court today appears to champion the idea that there is something *de minimis* about the Fourth

---

[3] I doubt anyone would be satisfied that an affidavit resting on a generic "gang member" profile, for example, could fulfill the requirements of the Fourth Amendment.

Amendment's requirements when the thing sought by a search authorization or warrant is child pornography. It is now effectively the case that signing up for a website related to that topic -- expressing an interest in it, from any location at all -- provides sufficient cause to search one's home or living quarters. 68 M.J. at 424-25. This reasoning requires three logical inferences: First, if the suspect is a member of an Internet group related to child pornography, he has access to a computer. Second, if he has access to a computer, it is in his home or living quarters. Third, membership in the group equates to downloading and possessing child pornography. The first inference makes sense, but the other two do not -- at least on the evidence presented to this magistrate.

People access the Internet at work, Internet cafés, public libraries, and myriad other places. The majority's logic is not and cannot be limited to one's home. Once we have held that an expressed interest in child pornography probably means you are viewing and secreting it *somewhere*, it seems equally sustainable to hold that the government is free to search for that pornography *anywhere*. This comes dangerously close to reviving the writs of assistance that were the impetus for enacting the Fourth Amendment in the first place. *See generally Boyd v. United States*, 116 U.S. 616, 625-26 (1886) (discussing the history of unreasonable searches and seizures prior to independence and how they influenced the Framers' view of the Fourth Amendment).

It is true that we are not the first court to treat child pornography this way. *Clayton*, 68 M.J. at 424-25 (citing *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006); *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005); *United States v. Froman*, 355 F.3d 882 (5th Cir. 2004); *United States v. Hutto*, 84 F. Appx. 6 (10th Cir. 2003)). But that others have joined our adventures does not make the course any less a folly. The better route is to continue to require, consistent with both M.R.E. 315(f) (2) and *Gates*, 462 U.S. at 238, some nexus between the items sought and the place the government wants to search. *Accord Higgins*, 557 F.3d at 390; *Frazier*, 423 F.3d at 533.

II. The Good Faith Exception

Because I do not believe the magistrate had a substantial basis for finding probable cause here, I must address the exception to the exclusionary rule for good faith reliance on a warrant, first announced by the Supreme Court in *United States v. Leon*, 468 U.S. 897, 922 (1984), and codified for the military justice system in M.R.E. 311 (b) (3). Under this rule:

> Evidence that was obtained as a result of an unlawful search or seizure may be used if:
>
> (A) The search or seizure resulted from an authorization to search, seize or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a

> search warrant or arrest warrant issued by competent civilian authority;
>
> (B) The individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and
>
> (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the issuance of the authorization or warrant. Good faith shall be determined on an objective standard.

I do not believe this exception saves the search here because reliance on a warrant is not in good faith "[w]here the magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *United States v. Carter*, 54 M.J. 414, 420 (C.A.A.F. 2001) (citation and quotation marks omitted). If government agents falsely or recklessly inform a magistrate, courts cannot allow those same agents to paper over their untruths with an exception meant to protect generally blameless actors.

At least one other court has held that:

> [T]he necessity of a nexus between the suspected criminal activity and the particular place to be searched is so well established that in the absence of such a connection, "the affidavit and resulting warrant are so lacking in indicia of

> probable cause as to render official belief in its existence entirely unreasonable."

Poolaw v. Marcantel, 565 F.3d 721, 734 (10th Cir. 2009) (quoting *United States v. Gonzales*, 399 F.3d 1225, 1231 (10th Cir. 2005)) . This is an argument that we have not yet addressed, but it is apparent even under our already-existing case law that the good faith exception does not save the search authorization here.

The affiant in this case knew that *no* pornography had been discovered on *any* Army computer, let alone Appellant's computer. Despite this fact, she included in her affidavit a statement unambiguously linking Appellant to already-discovered pornography: "The Camp Arifjan CID Office is currently conducting the discovery of apparent child pornography located within one of the Coalition Forces Land Component Command (CFLCC), CAKU, computers and the suspected login user is LTC Charles J. CLAYTON." Any reasonable law enforcement agent would know that a linkage between a suspect and contraband would be extremely important to a magistrate's decision to issue a search authorization. To indicate such a linkage without explaining to the magistrate precisely what she claims to have meant -- that the Criminal Investigation Command (CID) suspected "a person" within CFLCC -- shows a reckless disregard for the truth of the information before the

magistrate,[4] and CID therefore could not rely on the search authorization in good faith. *Cf. Wilson v. Russo*, 212 F.3d 781, 788 (3d Cir. 2000) ("[O]missions are made with reckless disregard if an officer withholds a fact in his ken that 'any reasonable person would have known ... was the kind of thing the judge would wish to know.'" (*quoting United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993)); *United States v. Cowgill*, 68 M.J. at 392-93 (C.A.A.F. 2010) (plurality opinion) (determining affiant acted with reckless disregard for the truth where, when asked a question by the magistrate that affiant did not know answer to, affiant gave magistrate what he assumed to be correct answer (it was incorrect) without either telling magistrate he was not sure or checking to make sure that the answer was, in fact, correct).

III. Conclusion

I would reverse the United States Army Court of Criminal Appeals. I respectfully dissent.

---

[4] This conclusion might be different if the false statement had been made orally, where a slip of the tongue was possible, and not in a written affidavit where the affiant could review the language to make sure it said precisely what she wanted it to say.